Chapter XVII

Trends in Information Assurance

Introduction

In Chapter I, we discussed the global status of information security. Based on the findings of the report *The Global State of Information Security 2005*, a worldwide study by CIO, CSO, and PricewaterhouseCoopers (PwC) in the *CSO Online Magazine* (Berinato, 2005), we outlined the problems individuals, organizations, and nations are facing to keep information secure.

Throughout the book, we set out to discuss what we think are ways to secure an information infrastructure that is secure for everyone. In particular, we focused on three areas:

Copyright © 2008, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
1. creation of an ethical or value framework for all users of the information technology
2. development and use of protocols and best practices that will enhance the security of the information infrastructure
3. enacting and enforcing a legal framework to strengthen the value system and act as a deterrent to the abuse of the information infrastructure

In each one of these areas, we have discussed a variety of approaches also surveying the latest tools and best practices. In this last chapter, we want to look back to Chapter I, given what we now know, and reflect on what is currently being done in the regulatory and policy framework on a global scale, and we also will speculate on what is likely to happen in some areas of information assurance.

Global Information Assurance

Initiatives and Trends

The growth of information has given a boost to businesses and enterprises as they have harnessed information technology for both the security and fat profits of their businesses. As the use of information technology becomes mainstreamed in businesses and in our day-to-day activities, both security and risk management have become individual, business, and national concerns. Every individual, enterprise, and government now needs reliable and secure information to carry out pertinent duties and responsibilities. In businesses, secure information is needed to reduce risk and protect systems and networks.

To help everyone using information, especially enterprises, increase information security awareness and needs, governments and security organizations are developing and continuously updating regulatory and policy frameworks. One way of doing this is through the development of effective information controls. An information control is a policy, a procedure, a practice, or an organizational structure designed to provide reasonable information assurance to achieve a stated objective. Neither technology nor policies and legislations alone offer any effective defense for an information system. Because of this realization, individuals, enterprises, and governments are relying more and